Preface

The third successful completion of the INDOCRYPT conference series marks the acceptance of the series by the international research community as a forum for presenting high-quality research. It also marks the coming of age of cryptology research in India.

The authors for the submitted papers were spread across 21 countries and 4 continents, which goes a long way to demonstrate the international interest and visibility of INDOCRYPT. In the previous two conferences, the submissions from India originated from only two institutes; this increased to six for the 2002 conference. Thus INDOCRYPT is well set on the path to achieving two main objectives – to provide an international platform for presenting high-quality research and to stimulate cryptology research in India.

The opportunity to serve as a program co-chair for the third INDOCRYPT carries a special satisfaction for the second editor. Way back in 1998, the scientific analysis group of DRDO organized a National Seminar on Cryptology and abbreviated it as NSCR. On attending the seminar, the second editor suggested that the conference name be changed to INDOCRYPT. It is nice to see that this suggestion was taken up, giving us the annual INDOCRYPT conference series. Of course, the form, character, and execution of the conference series was the combined effort of the entire Indian cryptographic community under the dynamic leadership of Bimal Roy.

There were 75 submissions to INDOCRYPT 2002, out of which one was withdrawn and 31 were accepted. The invited talks were especially strong. Vincent Rijmen of AES fame gave a lecture on the design strategy for the recently accepted AES standard. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena recently achieved a breakthrough by obtaining a polynomial time deterministic algorithm for primality testing. This was presented at an invited talk by the authors. GuoZhen Xiao, an eminent researcher in the theory of sequences and Boolean functions, presented a lecture on efficient algorithms for computing the linear complexity of sequences.

The reviewing process for INDOCRYPT was very stringent and the schedule was very tight. The program committee did an excellent job in reviewing the papers and selecting the final papers for presentation. These proceedings include the revised versions of the selected papers. Revisions were not checked and the authors bear the full responsibility for the contents of the respective papers.

Program committee members were assisted in the review process by external reviewers. The list of external reviewers is included in the proceedings. Our thanks go to all the program committee members and the external reviewers who put in their valuable time and effort in providing important feedback to the authors.

Organizing the conference involved many individuals. We would like to thank the general chairs V.P. Gulati and M. Vidyasagar for taking care of the actual
hosting of the conference. They were ably assisted by the organizing committee, whose names are included in the proceedings. Additionally, we would like to thank Kishan Chand Gupta, Sandeepan Chowdhury, Subhasis Pal, and Amiya Kumar Das for substantial help on different aspects of putting together this proceedings in its final form. Finally we would like to thank Springer-Verlag for active cooperation and timely production of the proceedings.

December 2002

Alfred Menezes
Palash Sarkar
INDOCRYPT 2002 was organized by the Institute for Development and Research in Banking Technology (IDRBT) and is an annual event of the Cryptology Research Society of India.

**General Co-chairs**

Ved Prakash Gulati  
IDRBT, Hyderabad, India

M. Vidyasagar  
Tata Consultancy Services, Hyderabad, India

**Program Co-chairs**

Alfred Menezes  
University of Waterloo, Canada

Palash Sarkar  
Indian Statistical Institute, India

**Program Committee**

Akshai Aggarwal  
University of Windsor, Canada

Manindra Agrawal  
Indian Institute of Technology, India

V. Arvind  
Institute of Mathematical Sciences, India

Simon Blackburn  
Royal Holloway, University of London, UK

Colin Boyd  
Queensland University of Technology, Australia

ZongDuo Dai  
Academia Sinica, China

Anand Desai  
NTT MCL, USA

Ved Prakash Gulati  
IDRBT, India

Anwar Hasan  
University of Waterloo, Canada

Sushil Jajodia  
George Mason University, USA

Charanjit Jutla  
IBM, USA

Andrew Klapper  
University of Kentucky, USA

Neal Koblitz  
University of Washington, USA

Kaoru Kurosawa  
Ibaraki University, Japan

Chae Hoon Lim  
Sejong University, Korea

Subhamoy Maitra  
Indian Statistical Institute, India

C.E. Veni Madhavan  
Indian Institute of Science, India

Alfred Menezes  
University of Waterloo, Canada

Rei Safavi-Naini  
University of Wollongong, Australia

David Pointcheval  
ENS Paris, France

Bart Preneel  
Katholieke Universiteit Leuven, Belgium

A.K. Pujari  
University of Hyderabad, India

Jaikumar Radhakrishnan  
Tata Institute of Fundamental Research, India

Bimal Roy  
Indian Statistical Institute, India

Palash Sarkar  
Indian Statistical Institute, India

Vijay Varadharajan  
Macquarie University, Australia

Stefan Wolf  
University of Montreal, Canada

Chaoping Xing  
National University of Singapore, Singapore

Amr Youssef  
Cairo University, Egypt
VIII  Organization

Organizing Committee

S. Sankara Subramanian  IDRBT, India  
Rajesh Nambiar  TCS, India  
V. Visweswar  IDRBT, India  
Ashutosh Saxena  IDRBT, India  
V. Ravi Sankar  IDRBT, India  
B. Kishore  TCS, India  

External Referees

Kazumaro Aoki  Michael Jacobs  Selwyn Russell  
Alexandra Boldyreva  Rahul Jain  Takeshi Shimoyama  
Shiping Chen  Shaoquan Jiang  M.C. Shrivastava  
Olivier Chevassut  Meena Kumari  Jason Smith  
Sandeepan Choudhury  Yingjiu Li  Alain Tapp  
Tammy K. Das  Sin’ichiro Matsuo  Ayineedi Venkateswarlu  
Matthias Fitzi  Mridul Nandi  Lingyu Wang  
Steven Galbraith  Laxmi Narain  Bogdan Warinschi  
Sugata Gangopadhyaya  Satomi Okazaki  Yiqun Lisa Yin  
Craig Gentry  Kapil Hari Paranjape  Sencun Zhu  
Indivar Gupta  Rajesh Pillai  
Alejandro Hevia  Matt Robshaw

Sponsoring Institutions

Acer India Pvt. Ltd., Bangalore  
Cisco Systems India Pvt. Ltd., New Delhi  
e-commerce magazine, New Delhi  
HP India, New Delhi  
IBM India Ltd., Bangalore  
Infosys Technologies Ltd., Bangalore  
Rainbow Information Technologies Pvt. Ltd. New Delhi  
Society for Electronic Transactions and Security, New Delhi  
Tata Consultancy Services, Mumbai
Table of Contents

Invited Talks

Security of a Wide Trail Design ..................................................1
Joan Daemen and Vincent Rijmen

Fast Algorithms for Determining the Linear Complexity
of Period Sequences ...............................................................12
Guozhen Xiao and Shimin Wei

Symmetric Ciphers

A New Class of Stream Ciphers Combining LFSR and FCSR Architectures 22
François Arnault, Thierry P. Berger, and Abdelkader Necer

Slide Attack on Spectr-H64 .....................................................34
Selçuk Kavut and Melek D. Yücel

On Differential Properties of Pseudo-Hadamard Transform
and Related Mappings (Extended Abstract) ..................................48
Helger Lipmaa

New Public-Key Schemes

A Variant of NTRU with Non-invertible Polynomials .......................62
William D. Banks and Igor E. Shparlinski

Tree Replacement and Public Key Cryptosystem .............................71
S.C. Samuel, D.G. Thomas, P.J. Abisha, and K.G. Subramanian

Foundations

Never Trust Victor:
An Alternative Resettable Zero-Knowledge Proof System ..................79
Olaf Müller and Michael Nüsken

Asynchronous Unconditionally Secure Computation:
An Efficiency Improvement .....................................................93
B. Prabhu, K. Srinathan, and C. Pandu Rangan
Table of Contents

Public-Key Infrastructures

QPKI: A QoS-Based Architecture for Public-Key Infrastructure (PKI) .... 108
Ravi Mukkamala

Towards Logically and Physically Secure Public-Key Infrastructures ...... 122
Kapali Viswanathan and Ashutosh Saxena

Fingerprinting and Watermarking

Cryptanalysis of Optimal Differential Energy Watermarking (DEW) and a Modified Robust Scheme ................................. 135
Tanmoy Kanti Das and Subhamoy Maitra

A 2-Secure Code with Efficient Tracing Algorithm ...................... 149
Vu Dong Tô, Reihaneh Safavi-Naini, and Yejing Wang

Reed Solomon Codes for Digital Fingerprinting .......................... 163
Ravi Sankar Veerubhotla, Ashutosh Saxena, and Ved Prakash Gulati

Public-Key Protocols

A Note on the Malleability of the El Gamal Cryptosystem .............. 176
Douglas Wikström

Authentication of Concat Communication ................................. 185
Mohamed Al-Ibrahim, Hossein Ghodosi, and Josef Pieprzyk

Self-certified Signatures .................................................. 199
Byoungcheon Lee and Kwangjo Kim

Identity Based Authenticated Group Key Agreement Protocol ........ 215
D. Nalla and K.C. Reddy

Boolean Functions

Construction of Cryptographically Important Boolean Functions ....... 234
Soumen Maity and Thomas Johansson

Evolving Boolean Functions Satisfying Multiple Criteria .............. 246
John A. Clark, Jeremy L. Jacob, Susan Stepney, Subhamoy Maitra, and William Millan

Further Results Related to Generalized Nonlinearity .................... 260
Sugata Gangopadhyay and Subhamoy Maitra
Table of Contents

Efficient and Secure Implementations

Modular Multiplication in $GF(p^k)$ Using Lagrange Representation ........ 275
Jean-Claude Bajard, Laurent Imbert, and Christophe Nègre

Speeding up the Scalar Multiplication in the Jacobians
of Hyperelliptic Curves Using Frobenius Map .......................... 285
YoungJu Choie and Jong Won Lee

Improved Elliptic Curve Multiplication Methods Resistant
against Side Channel Attacks ............................................ 296
Tetsuya Izu, Bodo Möller, and Tsuyoshi Takagi

Applications

The Design and Implementation of Improved Secure Cookies
Based on Certificate .......................................................... 314
Jong-Phil Yang and Kyung-Hyune Rhee

A Certified E-mail System with Receiver's Selective
Usage of Delivery Authority ............................................ 326
Kenji Imamoto and Kouichi Sakurai

Spending Offline Divisible Coins with Combining Capability .......... 339
Eikoh Chida, Yosuke Kasai, Masahiro Mambo, and Hiroki Shizuya

Efficient Object-Based Stream Authentication .......................... 354
Yongdong Wu, Di Ma, and Changsheng Xu

Anonymity

The Security of a Mix-Center
Based on a Semantically Secure Cryptosystem .......................... 368
Douglas Wikström

New Identity Escrow Scheme for Anonymity Authentication .......... 382
Yong-Ho Lee, Im-Yeong Lee, and Hyung-Woo Lee

Secret Sharing and Oblivious Transfer

On Unconditionally Secure Distributed Oblivious Transfer .......... 395
Ventzislav Nikov, Svetla Nikova, Bart Preneel, and Joos Vandewalle

Non-perfect Secret Sharing over General Access Structures .......... 409
K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan

On Distributed Key Distribution Centers
and Unconditionally Secure Proactive Verifiable Secret
Sharing Schemes Based on General Access Structure .............. 422
Ventzislav Nikov, Svetla Nikova, Bart Preneel, and Joos Vandewalle

Author Index ................................................................. 437
Table of Contents
**Author Index**

<table>
<thead>
<tr>
<th>Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abisha, P.J.</td>
<td>71</td>
</tr>
<tr>
<td>Al-Ibrahim, Mohamed</td>
<td>185</td>
</tr>
<tr>
<td>Arnault, François</td>
<td>22</td>
</tr>
<tr>
<td>Bajard, Jean-Claude</td>
<td>275</td>
</tr>
<tr>
<td>Banks, William D.</td>
<td>62</td>
</tr>
<tr>
<td>Berger, Thierry P.</td>
<td>22</td>
</tr>
<tr>
<td>Chida, Eikoh</td>
<td>339</td>
</tr>
<tr>
<td>Choi, YoungJu</td>
<td>285</td>
</tr>
<tr>
<td>Clark, John A.</td>
<td>246</td>
</tr>
<tr>
<td>Daemen, Joan</td>
<td>1</td>
</tr>
<tr>
<td>Das, Tannoy Kanti</td>
<td>135</td>
</tr>
<tr>
<td>Gangopadhyay, Sugata</td>
<td>260</td>
</tr>
<tr>
<td>Ghodosi, Hossein</td>
<td>185</td>
</tr>
<tr>
<td>Gulati, Ved Prakash</td>
<td>163</td>
</tr>
<tr>
<td>Imamoto, Kenji</td>
<td>326</td>
</tr>
<tr>
<td>Imbert, Laurent</td>
<td>275</td>
</tr>
<tr>
<td>Izu, Tetsuya</td>
<td>296</td>
</tr>
<tr>
<td>Jacob, Jeremy L.</td>
<td>246</td>
</tr>
<tr>
<td>Johansson, Thomas</td>
<td>234</td>
</tr>
<tr>
<td>Kasai, Yosuke</td>
<td>339</td>
</tr>
<tr>
<td>Kavut, Selçuk</td>
<td>34</td>
</tr>
<tr>
<td>Kim, Kwangjo</td>
<td>199</td>
</tr>
<tr>
<td>Lee, Byoungcheon</td>
<td>199</td>
</tr>
<tr>
<td>Lee, Hyung-Woo</td>
<td>382</td>
</tr>
<tr>
<td>Lee, Im-Yeong</td>
<td>382</td>
</tr>
<tr>
<td>Lee, Jong Won</td>
<td>285</td>
</tr>
<tr>
<td>Lee, Yong-Ho</td>
<td>382</td>
</tr>
<tr>
<td>Lipmaa, Helger</td>
<td>48</td>
</tr>
<tr>
<td>Ma, Di</td>
<td>354</td>
</tr>
<tr>
<td>Maitra, Subhamoy</td>
<td>135, 246, 260</td>
</tr>
<tr>
<td>Maity, Soumen</td>
<td>234</td>
</tr>
<tr>
<td>Mambo, Masahiro</td>
<td>339</td>
</tr>
<tr>
<td>Millan, William</td>
<td>246</td>
</tr>
<tr>
<td>Möller, Bodo</td>
<td>296</td>
</tr>
<tr>
<td>Müller, Olaf</td>
<td>79</td>
</tr>
<tr>
<td>Mukkamala, Ravi</td>
<td>108</td>
</tr>
<tr>
<td>Nalla, Divya</td>
<td>215</td>
</tr>
<tr>
<td>Necer, Abdelkader</td>
<td>22</td>
</tr>
<tr>
<td>Negré, Christophe</td>
<td>275</td>
</tr>
<tr>
<td>Nikov, Ventsislav</td>
<td>395, 422</td>
</tr>
<tr>
<td>Nikova, Svetla</td>
<td>395, 422</td>
</tr>
<tr>
<td>Nüksen, Michael</td>
<td>79</td>
</tr>
<tr>
<td>Pieprzyk, Josef</td>
<td>185</td>
</tr>
<tr>
<td>Prabhu, B.</td>
<td>93</td>
</tr>
<tr>
<td>Preneel, Bart</td>
<td>395, 422</td>
</tr>
<tr>
<td>Rajan, N. Tharani</td>
<td>409</td>
</tr>
<tr>
<td>Rangan, C. Pandu</td>
<td>93, 409</td>
</tr>
<tr>
<td>Reddy, K.C.</td>
<td>215</td>
</tr>
<tr>
<td>Rhee, Kyung-Hyune</td>
<td>314</td>
</tr>
<tr>
<td>Rijmen, Vincent</td>
<td>1</td>
</tr>
<tr>
<td>Safavi-Naini, Reihaneh</td>
<td>149</td>
</tr>
<tr>
<td>Sakurai, Kouichi</td>
<td>326</td>
</tr>
<tr>
<td>Samuel, S.C.</td>
<td>71</td>
</tr>
<tr>
<td>Saxena, Ashutosh</td>
<td>122, 163</td>
</tr>
<tr>
<td>Shizuya, Hiroki</td>
<td>339</td>
</tr>
<tr>
<td>Shparlinski, Igor E.</td>
<td>62</td>
</tr>
<tr>
<td>Srinathan, K.</td>
<td>93, 409</td>
</tr>
<tr>
<td>Stepney, Susan</td>
<td>246</td>
</tr>
<tr>
<td>Subramanian, K.G.</td>
<td>71</td>
</tr>
<tr>
<td>Takagi, Tsuyoshi</td>
<td>296</td>
</tr>
<tr>
<td>Thomas, D.G.</td>
<td>71</td>
</tr>
<tr>
<td>Tô, Vu Dong</td>
<td>149</td>
</tr>
<tr>
<td>Vandewalle, Joos</td>
<td>395, 422</td>
</tr>
<tr>
<td>Veerubhotla, Ravi Sankar</td>
<td>163</td>
</tr>
<tr>
<td>Viswanathan, Kapali</td>
<td>122</td>
</tr>
<tr>
<td>Wang, Yejing</td>
<td>149</td>
</tr>
<tr>
<td>Wei, Shimin</td>
<td>12</td>
</tr>
<tr>
<td>Wikström, Douglas</td>
<td>176, 368</td>
</tr>
<tr>
<td>Wu, Yongdong</td>
<td>354</td>
</tr>
<tr>
<td>Xiao, Guozhen</td>
<td>12</td>
</tr>
<tr>
<td>Xu, Changsheng</td>
<td>354</td>
</tr>
<tr>
<td>Yang, Jong-Phil</td>
<td>314</td>
</tr>
<tr>
<td>Yücel, Melek D.</td>
<td>34</td>
</tr>
</tbody>
</table>